Security Attacks in Mobile Ad-hoc Networks – A Literature Survey

T. Navaneethan[#1], M. Lalli[*2]

[#1] School of Computer Science and Engineering, Bharathidasan University, Trichy

[*2] School of Computer Science and Engineering, Bharathidasan University, Trichy

[#1] navaneethanvel@gmail.com

[*2] lalli_gss@yahoo.co.in

ABSTRACT:

A MANET (Mobile Ad-hoc Network) is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. A MANET is a most promising and rapidly growing technology and it have become a very popular research topic in recent years. Wireless networks are vulnerable to security attacks, which allows for many other forms of attacks on the networks. By providing communications in the absence of a fixed infra-structure MANETs are an attractive technology for many applications such as rescue operations, tactical operations, environmental monitoring, conferences, and the like. Security is a major concern for protected communication between mobile nodes in an unfriendly environment. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various attacks such as spoofing, black hole, worm hole, flooding, eavesdropping and so on. This paper provides different kinds of attacks in MANET.

Keywords: MANET, Vulnerability, Security attacks, Active attacks, Passive attacks

1. INTRODUCTION:

MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that’s why it is sometimes referred to as an “infrastructure less” network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad hoc network is self organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. It includes Military Battlefield, Sensor Networks, Medical Service and Personal Area Network. Security solutions are important issues for MANET, especially for those selecting sensitive applications, have to meet the following design goals while addressing the above challenges. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to security attacks.

Routing is necessary in MANET, but it create problem and Challenges as compared to the routing in fixed infrastructure. The problem in routing is due to the rapidly changes in the topology of the nodes and the devices. There are two type of routing

1. Proactive
2. Reactive.

In proactive routing, there is a fixed topology and use a single protocol. OLSR and DSDV are the proactive routing protocol.

In reactive routing, there is several protocol are used between the two devices and the type of topology is change according to the condition. AODV and DSR are the reactive routing protocol.

2. SECURITY SERVICES:

Based on the characteristics of MANETs and a variety of attacks that we have described in the previous sections, we are now in a position to discuss the security services that are usually expected to be provided by the security mechanism in MANETs. Security services can be categorized into: authentication, access control, confidentiality, integrity, non-repudiation, and availability.

Authentication: Authentication is the ability to verify a user's identity in an association and to assure the recipient that the message is from the source that it claims to be. Authentication is a fundamental mechanism to support access control.

Access Control: Access Control is the ability to limit and control access to devices and applications via communication links. A user trying to gain access to the resource is first authenticated and then the corresponding access rights are granted.

Confidentiality: Confidentiality ensures that the information transmitted over the network is unreadable to unauthorized users or nodes. Confidentiality can be achieved by using various encryption techniques.

Integrity: Integrity is to be able to keep the data transmitted from being illegally modified or destroyed during the transmission.

Non-repudiation: Non-repudiation guarantees that neither the sender nor the receiver of a message is able to deny the transmission.

Availability: Availability is to keep the network service or resources available to legitimate users. It ensures the survivability of the network despite malicious incidents.

3. MANET VULNERABILITIES:

Wireless Links:

First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Unlike wired networks, attackers do not need physical access to the network to carry out these attacks. Furthermore wireless networks typically have lower bandwidths than wired networks. Attackers can exploit this feature, consuming network bandwidth with ease to prevent normal communication among nodes.

Dynamic Topology:

MANET nodes can leave and join the network, and move independently. As a result the network topology can change frequently. It is hard to differentiate normal behavior of the network from anomaly/malicious behavior in this dynamic environment. For example, a node sending disruptive routing information can be a malicious node, or else simply be using outdated information in good faith. Moreover mobility of nodes means that we cannot assume nodes, especially critical ones (servers, etc.), are secured in locked cabinets as in wired networks. Nodes with inadequate physical protection may often be at risk of being captured and compromised.

Cooperativeness:

Routing algorithms for MANETs usually assume that nodes are cooperative and nonmalicious. As a result, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications. For example, a node can pose as a neighbor to other nodes and participate in collective decision-making mechanisms, possibly affecting networking significantly.

Lack of a Clear Line of Defense:

MANETs do not have a clear line of defense; attacks can come from all directions [27]. The boundary that separates the inside network from the outside world is not very clear on MANETs. For example, there is no well defined place where we can deploy our traffic monitoring, and access control mechanisms. Whereas all traffic goes through switches, routers, or gateways in wired networks, network information in MANETs is distributed across nodes that can only see the packets sent and received in their transmission range.

***Limited Resources*:**

Resource constraints are a further vulnerability. There can be a variety of devices on MANETs, ranging from laptops to handheld devices such as PDAs and mobile phones. These will generally have different computing and storage capacities that can be the focus of new attacks. For example, mobile nodes generally run on battery power.

4. SECURITY ATTACKS IN MANETS:

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types.

A. Internal Attacks Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more trusted nodes. The wrong routing information generated by compromised nodes or malicious nodes are difficult to identify. This can be due to the compromised nodes are able to generate the valid signature using their private keys.

B. External attacks These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories:

1) Passive attacks MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized “listening” to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. Detection of such type of attacks is difficult since the operation of network itself doesn’t get affected. In order to overcome this type of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

2) Active Attacks Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. The active attacks are generally launched by compromised nodes or malicious nodes. Malicious nodes change the routing information by advertising itself as having shortest path to the destination.

Table 1: Security Attacks Classification

Passive Attacks	Eavesdropping, traffic analysis, monitoring
Active Attacks	Dropping, modification, fabrication, timing

5. PASSIVE ATTACKS:

In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping, traffic analysis and monitoring.

Eavesdropping Attacks:

Eavesdropping attack is also known as disclosure attacks, are passive attacks by external or internal nodes. The attacker can analyze broadcast messages to reveal some useful information about the network. The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium. Majorities of wireless communication use RF spectrum and broadcast by nature. Message transmitted can be eavesdropped and fake message can be injected into network.

Traffic Analysis:

Traffic analysis is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols, or seek to provoke communication between nodes. Attackers may employ techniques such as RF direction finding, traffic rate analysis, and time-correlation monitoring. Traffic analysis in ad hoc networks may reveal:

- the existence and location of nodes;
- the communications network topology;
- the roles played by nodes;
- the current sources and destination of communications; and
- the current location of specific individuals or functions (e.g. if the commander issues a daily briefing at 10am, traffic analysis may reveal a source geographic location).

Monitoring:

It can be developed to identify the communication parties and functionality which could provide information to launch further attacks .It is not specific to MANET, other wireless network such as cellular, satellite and WLAN also suffer from these potential vulnerabilities Monitoring is a passive attack in which attacker can see the confidential data, but he cannot change the data or cannot modify the data.

6. ACTIVE ATTACKS:

These attacks cause unauthorized state changes in the network such as denial of service, modification of packets, and the like. These attacks are generally launched by users or nodes with authorization to operate within the network. We classify active attacks into four groups: dropping, modification, fabrication, and timing attacks. It should be noted that an attack can be classified into more than one group.

Dropping Attacks:

Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point. Most of routing protocol has no mechanism to detect whether data packets have been forwarded or not.

Modification Attacks:

Sinkhole attacks are the example of modification attacks. These attacks modify packets and disrupt the overall communication between network nodes. In sinkhole attack, the compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node than capture important routing information and uses it for further attacks such as dropping and selective forwarding attacks.

Fabrication Attacks:

In fabrication attack, the attacker send fake message to the neighbouring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages.

Timing Attacks:

In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique.

Here we map the attacks (active or passive) with the layers

TABLE 2: Mapping of Attacks in each layer

Attacks	Passive Attacks	Active Attacks	Layer
Spoofing		Y	Network layer
Fabrication		Y	Multi-layer
Modification		Y	Multi-layer
Wormhole		Y	Network layer
Denial of service		Y	Multi- layer
Sinkhole		Y	Network layer
Sybil		Y	Network layer
Eavesdropping	Y		Physical layer
Traffic Analysis	Y		Data link layer
Monitoring	Y		Data link layer
Black hole		Y	Network layer
Rushing		Y	Multi-layer
Reply	Y		Multi-layer
Location Disclosure		Y	Network layer
Byzantine		Y	Network layer

7. OTHER ADVANCED ATTACKS:

More sophisticated and subtle routing attacks have been identified in recent research papers. The blackhole (or sinkhole), wormhole attack, Byzantine, and rushing attacks are the typical examples, which are described in detail below.

Wormhole Attack:

An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

Blackhole Attack:

The blackhole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrong doing.

Byzantine Attack:

A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

Rushing Attack:

Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure.

Resource Consumption Attack:

This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node

Location Disclosure Attack:

An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against MANET, is unsolved. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security sensitive scenarios.

Table 3: Security Attacks on each layer in MANET

Layer	**Attacks**
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping

8. CONCLUSION:

In this paper, we try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile adhoc network, which need to gain enough attention. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. The existence of these vulnerabilities has made it necessary to find some effective security solutions and protect the mobile ad hoc network from all kinds of security risks. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. On one hand, the security-sensitive applications of an ad-hoc networks require high degree of security on the other hand, adhoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks.

REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book *The Handbook of Ad Hoc Wireless Networks (chapter 1)* CRC Press LLC, 2003.

[2] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks ,(chapter 30)* CRC Press LLC, 2003.

[3] Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks"

[4] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey".

[5] Kamanshis Biswas and Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network".

[6] P. Michiardi, R. Molva, "*Ad hoc networks security,"* IEEE Press Wiley, New York, 2003.

[7] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M. "An Overview Of security Problems in MANET".

[8] Satyam Shrivastava, Sonali Jain, "A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network".

[9] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks".

[10] Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks".